CyberOps Associates v1.0 - Skills Assessment

Introduction

You have been hired as a junior security analyst. As part of your training, you were tasked to determine any malicious activity associated with the Pushdo trojan.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

- Evaluate event alerts using Squil and Kibana.
- Use Google search as a tool to obtain intelligence on a potential exploit.
- Use VirusTotal to upload and verify threat existence.

Content for this assessment was obtained from http://www.malware-traffic-analysis.net/ and is used with permission. We are grateful for the use of this material.

Required Resources

- Host computer with at least 8GB of RAM and 45GB of free disk space
- Latest version of Oracle VirtualBox
- Security Onion virtual machine requires 4GB of RAM using 25GB disk space
- Internet access

Instructions

Part 1: Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

Step 1: Verify the status of services

a. Log into Security Onion VM using with the username **analyst** and password **cyberops**.

b. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.

c. When the nsm service is ready, log into Sguil or Kibana with the username **analyst** and password **cyberops**.

Step 2: Gather basic information.

a. Identify time frame of the Pushdo trojan attack, including the date and approximate time.

b. List the alerts noted during this time frame associated with the trojan.

c. List the internal IP addresses and external IP addresses involved.

Part 2: Learn about the Exploit

In this part, you will learn more about the exploit.

Step 1: Infected host

a. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (**Hint**: NetworkMiner or internet search)

b. Based on the alerts, when (date and time in UTC) and how was the PC infected? (**Hint**: Enter the command **date** in the terminal to determine the time zone for the displayed time)

How did the malware infect the PC? Use an internet search as necessary.

Step 2: Examine the exploit.

a. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

b. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.

c. Examine other alerts associated with the infected host during this timeframe and record your findings

Step 3: Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.